



PCT/FR2004/002579

REC'D 17 DEC 2004

WIPO PCT

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 04 OCT. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75300 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11354*03

REQUÊTE EN DÉLIVRANCE page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 • 11 / 210502

REMISE DES PIÈCES DATE 17 OCT 2003 LIEU 75 INPI PARIS N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0312152 DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 17 OCT. 2003		2 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE CABINET BOETTCHER 22 rue du Général Foy 75008 PARIS	
Vos références pour ce dossier (facultatif) 3F-1247 CAS 258 GF			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
ou demande de certificat d'utilité initiale		N° _____ Date _____	
Transformation d'une demande de brevet européen		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Procédé de protection d'un algorithme cryptographique			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		SAGEM SA	
Prénoms			
Forme juridique		Société Anonyme	
N° SIREN		15 620 829 09	
Code APE-NAF			
Domicile ou siège	Rue	Le Ponant de Paris 27 rue Leblanc	
	Code postal et ville	75 015 PARIS	
	Pays	FRANCE	
Nationalité		française	
N° de téléphone (facultatif)		N° de télécopie (facultatif)	
Adresse électronique (facultatif)			
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page



BREVET D'INVENTION CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

REMISE DES PIÈCES DATE 17 OCT 2003 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0312152 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 W / 210502
6 MANDATAIRE (s'il y a lieu)		Les inventeurs sont nécessairement des personnes physiques	
Nom Prénom Cabinet ou Société N° de pouvoir permanent et/ou de lien contractuel		FRUCHARD et/ou ROBERT, JAUNEZ, LAVIALLE Guy et/ou Jean-Pierre, Xavier, Bruno CABINET BOETTCHER	
Adresse Rue Code postal et ville Pays		22 rue du Général Foy 75 010 18 PARIS FRANCE	
N° de téléphone (facultatif) N° de télécopie (facultatif) Adresse électronique (facultatif)			
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques	
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> Établissement immédiat <input type="checkbox"/> Établissement différé	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence): AG	
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		<input type="checkbox"/> Cochez la case si la description contient une liste de séquences	
Le support électronique de données est joint La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		<input type="checkbox"/> <input type="checkbox"/>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes			
11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) Guy FRUCHARD Mandataire CPI BREVET 92 1094		VISA DE LA PRÉFECTURE OU DE L'INPI RI ANCANER	

La présente invention concerne un procédé de protection d'un algorithme cryptographique.

ARRIERE PLAN DE L'INVENTION

5 On sait que la façon la plus efficace de conserver la confidentialité lors d'une transmission de données est de chiffrer les données au moyen d'un algorithme cryptographique.

10 A cet effet on connaît des dispositifs comportant une unité de traitement programmable associés à un fichier de configuration comportant un algorithme cryptographique personnalisé. L'entité réalisant l'algorithme cryptographique personnalisé est généralement différente de l'entité réalisant le dispositif utilisant l'algorithme cryptographique. Afin de protéger l'algorithme
15 cryptographique pendant le transport depuis son lieu d'élaboration jusqu'à son chargement dans le dispositif auquel il est destiné, on procède habituellement à un chiffrement de l'algorithme lui-même en utilisant une clé de protection. Sous cette forme chiffrée, l'algorithme
20 cryptographique ne peut être exécuté par le dispositif auquel il est destiné. Lors du chargement de l'algorithme cryptographique dans le dispositif auquel il est destiné, un déchiffrement est donc effectué dans l'unité de traitement en utilisant la clé de protection qui y a été communiquée par le fabricant du dispositif et introduite par
25 celui-ci dans l'unité de traitement. Le fabricant du dispositif ayant accès à la clé de protection, il est possible pour un fraudeur qui réussirait à obtenir d'une part l'algorithme cryptographique chiffré et d'autre part la clé détenue par le fabricant du dispositif, d'effectuer un déchiffrement de l'algorithme cryptographique lui permettant de reconstituer cet algorithme. En outre, après son déchiffrement l'algorithme n'est plus protégé de sorte qu'il est absolument nécessaire de disposer de
30 moyens de sécurité particuliers pour protéger l'unité de
35

traitement pendant l'exécution de l'algorithme.

OBJET DE L'INVENTION

Un but de l'invention est de proposer un procédé de protection d'un algorithme cryptographique y compris
5 lors de son exécution dans une unité de traitement sans qu'il soit nécessaire de faire intervenir le fabricant de l'unité de traitement.

BREVE DESCRIPTION DE L'INVENTION

En vue de la réalisation de ce but, on propose,
10 selon l'invention, un procédé de protection d'un algorithme cryptographique décomposable sous forme de polynômes initiaux à au moins deux variables et ayant un degré au moins égal à deux, le procédé comportant les étapes de réaliser des polynômes combinés, chacun obtenu à partir
15 d'au moins deux polynômes initiaux, et de mettre en œuvre les polynômes combinés dans l'unité de traitement.

Ainsi, la combinaison d'au moins deux polynômes initiaux ayant un degré au moins égal à deux, réalise un polynôme ayant un degré au moins égal à quatre dont il
20 est extrêmement difficile de retrouver les constituants en particulier lorsque le nombre de variables de ces polynômes est suffisamment important. L'algorithme ainsi transformé est donc protégé et peut donc être transmis avec un degré de sécurité satisfaisant. Par ailleurs, les
25 polynômes combinés sont directement exécutables au même titre que les polynômes initiaux. Aucune transformation n'est nécessaire lors de la configuration de l'unité de traitement de sorte que l'algorithme reste protégé pendant son exécution.

30 Selon une version avantageuse de l'invention, un effacement partiel de l'unité de traitement, et de la mémoire contenant le fichier de configuration lorsque la configuration est présente, est provoqué dans le cas d'une intrusion dans le dispositif. Dès l'instant où
35 quelques informations sont manquantes la difficulté de

reconstitution de l'algorithme est considérablement augmentée de sorte qu'un effacement partiel seulement suffit à protéger l'algorithme.

5 Selon un autre aspect avantageux de l'invention, le procédé comporte en outre l'étape de combiner chaque polynôme combiné avec une fonction, et de combiner le polynôme combiné suivant avec une fonction inverse. Cette transformation complémentaire augmente encore la difficulté de retrouver les polynômes initiaux sans toutefois
10 nuire au caractère exécutable du polynôme combiné en raison de l'élimination d'une fonction directe par la fonction inverse correspondante lors du passage d'un polynôme combiné au polynôme combiné suivant.

De préférence, la fonction combinée à chaque polynôme combiné est une fonction linéaire. Le degré du polynôme combiné reste alors inchangé, de sorte que l'espace pris en mémoire par le polynôme combiné reste lui-même inchangé.

DESCRIPTION DETAILLEE DE L'INVENTION

20 D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture de la description qui suit d'un mode de mise en œuvre particulier non limitatif de l'invention en relation avec la figure unique ci-jointe qui est un diagramme schématique illustrant le
25 procédé selon l'invention.

En référence à la figure, le procédé de protection d'un algorithme cryptographique selon l'invention est destiné à être mis en œuvre dans un dispositif de chiffrement 1 comportant de façon connue en soi un boîtier 2 dans lequel est disposée une mémoire volatile 3
30 destinée à contenir un fichier de configuration et reliée à une unité de traitement 4 configurable par le fichier de configuration pour effectuer un chiffrement de données introduites dans le dispositif.

35 Egalement de façon connue en soi, le dispositif 1

comporte un organe d'effacement 5 relié à la mémoire 3 et à l'unité de traitement 4, pour assurer en cas d'intrusion un effacement au moins partiel des informations qu'elles contiennent. A cet effet la mémoire et l'unité de traitement 4 sont de préférence volatiles de sorte qu'une interruption même brève de l'alimentation provoque un effacement partiel des informations contenues dans la mémoire et/ou l'unité de traitement.

Selon l'invention, l'algorithme cryptographique 6 qui est destiné à être introduit dans le fichier de configuration 3 est tout d'abord divisé selon un procédé connu en soi, selon des rondes représentées par des polynômes initiaux $P_1, P_2, P_3, P_4, \dots, P_i, P_{i+1}, \dots, P_{r-1}, P_r$, à plusieurs variables et ayant un degré au moins égal à deux. Les polynômes initiaux sont déterminés en utilisant différentes clés (sauf répétition au hasard), ou différentes sous-clés d'une même clé. Les clés ou les sous-clés peuvent être totalement intégrées aux polynômes ou constituer des variables supplémentaires au sein des polynômes. Les polynômes initiaux P_i sont ensuite combinés, deux par deux dans le mode de mise en œuvre illustré, selon une combinaison mathématique de fonctions, pour obtenir des polynômes combinés $Q_1 = P_2 \circ P_1, Q_2 = P_4 \circ P_3, \dots, Q_k = P_{i+1} \circ P_i, \dots, Q_{r/2} = P_r \circ P_{r-1}$. Lorsque les polynômes P_i ont un degré égal à deux, les polynômes combinés Q_k ainsi obtenus ont un degré égal à quatre.

Dans le mode de mise en œuvre préféré illustré, chaque polynôme Q_k est en outre combiné avec une fonction f_k , de préférence une fonction linéaire, et le polynôme combiné suivant est combiné de façon correspondante avec la fonction inverse f_k^{-1} , à l'exception bien entendu du premier et du dernier polynômes combinés qui ne sont combinés qu'avec une fonction directe pour l'un et une fonction inverse pour l'autre.

Avant son chargement dans la mémoire 3 sous forme

d'un fichier de configuration, l'algorithme cryptographique est donc représenté par les fonctions polynomiales $f_1 \circ Q_1, f_2 \circ Q_2 \circ f_1^{-1}, \dots, f_k \circ Q_k \circ f_{k-1}^{-1}, f_{k+1} \circ Q_{k+1} \circ f_k^{-1}, \dots, Q_{r/2} \circ f_{r/2-1}^{-1}$.

5 Bien entendu, l'invention n'est pas limitée au mode de mise en œuvre décrit et on peut y apporter des variantes de réalisation sans sortir du cadre de l'invention tel que défini par les revendications.

10 En particulier, bien que les rondes initiales aient été représentées sous forme d'un seul polynôme initial par ronde, chaque ronde peut contenir plusieurs polynômes initiaux. Les polynômes initiaux peuvent donc être combinés au sein d'une même ronde ou en combinant plusieurs rondes entre elles.

15 Bien que le procédé ait été décrit en relation avec un dispositif comprenant une unité de traitement 4 associée à une mémoire 3 destinée à recevoir l'algorithme sous forme d'un fichier de configuration, ce qui permet d'effectuer une modification de la configuration sans
20 avoir à effectuer un retour du dispositif en atelier, on peut prévoir une mise en œuvre directe de l'algorithme dans l'unité de traitement par une configuration de l'unité de traitement en atelier. Dans ce cas la configuration ne peut plus être modifiée sans un retour en atelier.
25

Bien que le procédé selon l'invention ait été décrit en combinant les polynômes initiaux deux à deux, il peut être nécessaire pour certains algorithmes de regrouper les polynômes élémentaires selon un nombre supérieur
30 à deux. Par exemple pour l'algorithme dénommé DES dans lequel les rondes sont entrelacées, il est nécessaire de combiner plus de deux polynômes initiaux pour obtenir des polynômes combinés exécutables de façon sûre selon le procédé décrit ci-dessus.

35 Bien que l'invention ait été décrite avec une

étape comprenant une combinaison avec une fonction et la fonction inverse, on peut prévoir de constituer le fichier de configuration simplement à partir des polynômes combinés Q_k .

- 5 Au lieu d'effectuer la combinaison des différents polynômes combinés Q_k avec des fonctions f_k différentes pour chacun des polynômes combinés Q_k comme décrit ci-dessus, on peut combiner chaque polynôme combiné avec la même fonction f puis avec la fonction inverse f^{-1} .

REVENDEICATIONS

1. Procédé de protection d'un algorithme cryptographique (6) en vue de son exécution dans un dispositif (1) comprenant une unité de traitement programmable (4), l'algorithme étant décomposable sous forme de polynômes initiaux (P_i) à au moins deux variables et ayant un degré au moins égal à deux, caractérisé en ce que le procédé comporte les étapes de réaliser des polynômes combinés (Q_k) chacun obtenu à partir d'au moins deux polynômes initiaux (P_i, P_{i+1}), et de mettre en œuvre les polynômes combinés (Q_k) dans l'unité de traitement programmable (4).

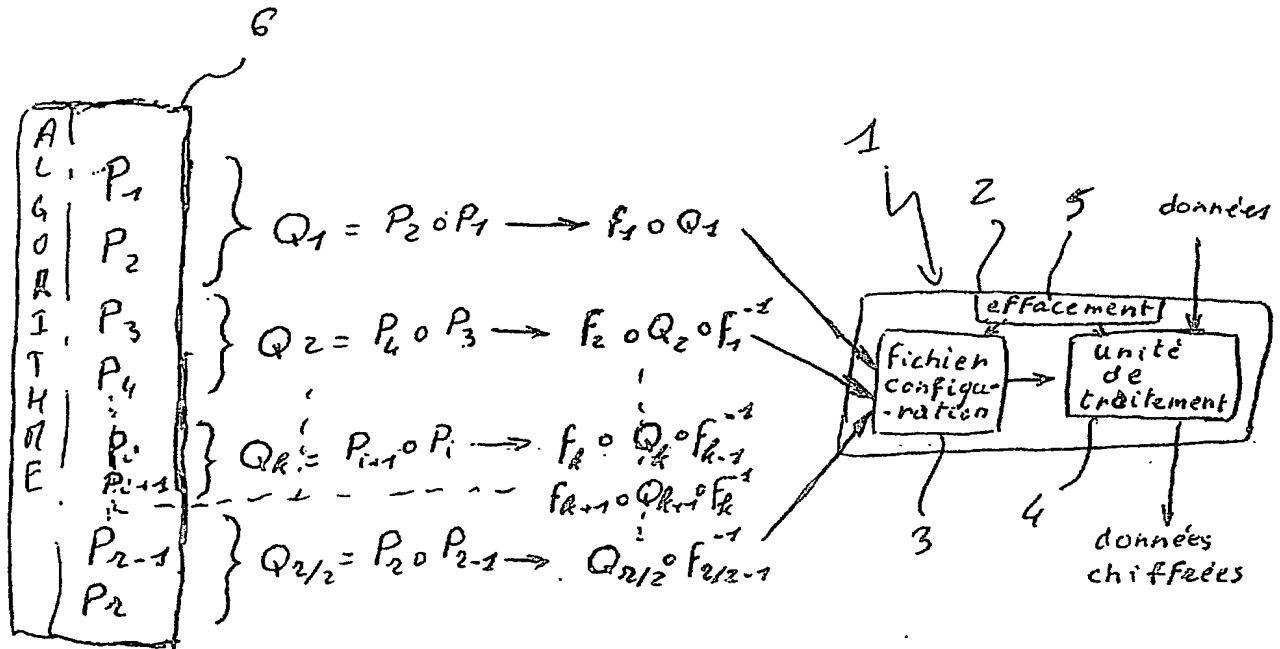
2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte en outre l'étape de mémoriser les polynômes combinés (Q_k) sous forme d'un fichier de configuration chargé dans une mémoire (3) associée à l'unité de traitement (4).

3. Procédé selon la revendication 2, caractérisé en ce que la mémoire (3) et l'unité de traitement programmable (4) sont associés à un organe d'effacement (5) provoquant, dans le cas d'une intrusion dans le dispositif, un effacement de l'unité de traitement (4), et un effacement de la mémoire (3) contenant le fichier de configuration lorsque la configuration est présente dans cette mémoire.

4. Procédé selon la revendication 1, caractérisé en ce qu'il comporte l'étape de combiner chaque polynôme combiné (Q_k) avec une fonction (f_k), et de combiner le polynôme combiné suivant (Q_{k+1}) avec une fonction inverse (f_k^{-1}).

5. Procédé selon la revendication 4, caractérisé en ce que la fonction (f_k) combinée à chaque polynôme combiné (Q_k) est une fonction linéaire.

4/4



Foi 1

287

Le Mandataire

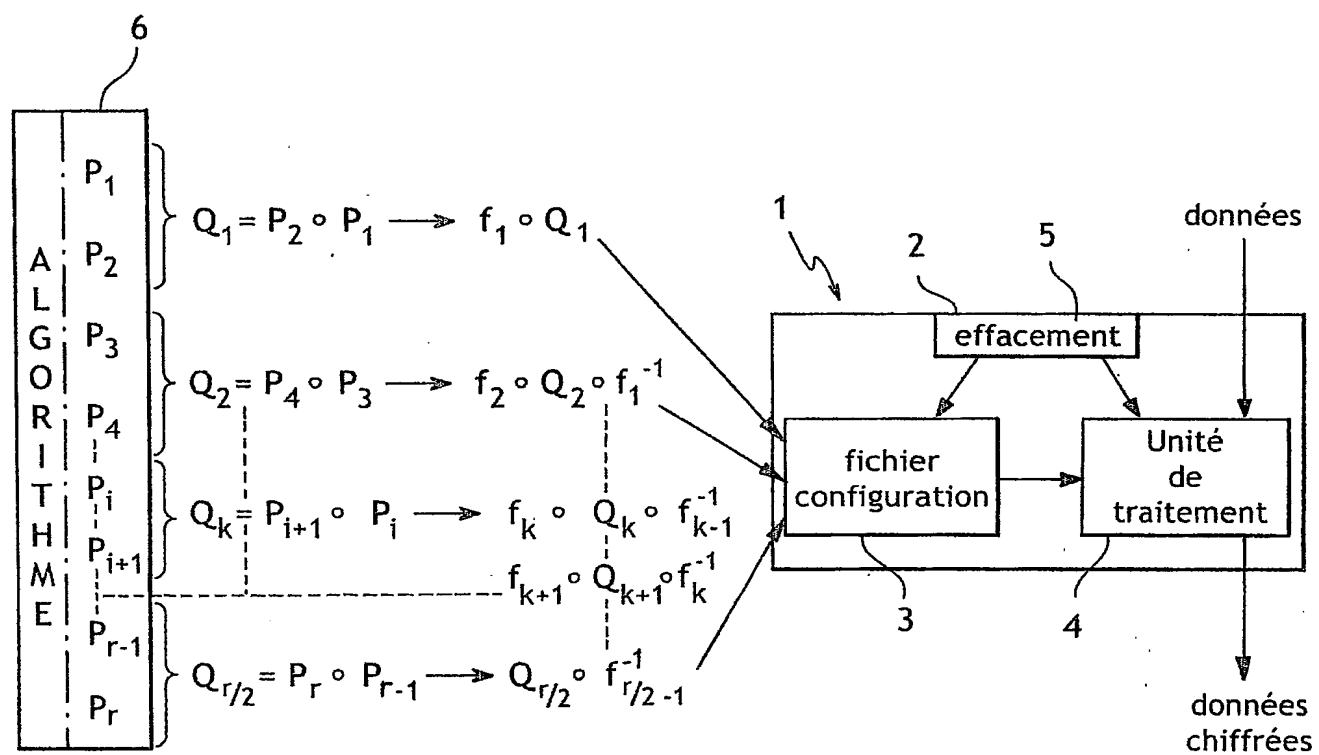


FIG.1



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75600 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1. / 1..

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 260899

Vos références pour ce dossier (facultatif)		3F-1247 CAS 258 GF	
N° D'ENREGISTREMENT NATIONAL		0312152	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
Procédé de protection d'un algorithme cryptographique			
LE(S) DEMANDEUR(S) :			
SAGEM SA			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		CARLIER	
Prénoms		Vincent	
Adresse	Rue	15 rue Buffon	
	Code postal et ville	91400	ORSAY (FRANCE)
Société d'appartenance (facultatif)			
Nom		CHABANNE	
Prénoms		Hervé	
Adresse	Rue	48 rue de la Marne	
	Code postal et ville	78200	MANTES LA JOLIE (FRANCE)
Société d'appartenance (facultatif)			
Nom		DOTTAX	
Prénoms		Emmanuelle	
Adresse	Rue	29, rue de la Fontaine au Roi	
	Code postal et ville	75011	PARIS (FRANCE)
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)			
PARIS, le 17 octobre 2003 Guy FRUCHARD Mandataire CPI BREVET 92 1094			

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record.**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.